Blue Cloud of Death: Red Teaming Azure

BSides Denver Presentation on May 11 2018

On-demand IT services are being publicized as the “new normal”, but often times these services are misunderstood and hence misconfigured by engineers which can frequently enable red teams to gain, expand, and persist access within Azure environments.

In this talk we will dive into how Azure services are commonly breached (e.g. discovering insecure blob storage), and then show how attackers are pivoting between the data & control planes (e.g. mounting hard disks, swapping keys, etc...) to expand access. Finally we will demonstrate some unique techniques for persisting access within Azure environments for prolonged periods of time.

Bryce Kunz (@TweekFawkes) is an Information Security Researcher located in Salt Lake City, Utah. Bryce currently leads the security offensive testing of Adobe's Marketing Cloud SaaS infrastructure via researching and developing custom exploits for web applications and other cloud based technologies. As a security professional, Bryce has spent time at various agencies (i.e. NSA, DoD, DHS, CBP) focusing on vulnerability research, penetration testing, and incident response. Bryce received an MBA from a NSA designated "Center of Excellence" Idaho State University (ISU) program with an emphasis in Information Assurance (IA) on a full academic scholarship from the National Science Foundation (NSF). Bryce holds numerous certifications (e.g. OSCP, CISSP, ...) and has spoken at various security conferences (i.e. DerbyCon, etc...).